Google

Web   Images   Video   News   Maps   more »

| data encryption standard | | Search | Advanced Search
Preferences |

Web

Results **1 - 10** of about **13,600,000** for data encryption standard . (0.12 seconds)

Data encryption standard
Sponsored Link
www.FindWhitePapers.com   Download Free IT White Papers about
Email Security, **Encryption** and More

Tip: Save time by hitting the return key instead of clicking on "search"

FIPS 46-2 - (DES), Data Encryption Standard
The **Data Encryption Standard** (DES) specifies a FIPS approved
cryptographic ... Federal Information Processing **Standard** (FIPS) 46-2,
Data Encryption Standard ...
www.itl.nist.gov/fipspubs/fip46-2.htm - 46k - Cached - Similar pages

Data Encryption Standard - Wikipedia, the free encyclopedia
The **data encryption standard** (DES) and its strength against attacks.
... CRYPTO 1994: pp1-11; National Bureau of **Standards, Data
Encryption Standard,** ...
en.wikipedia.org/wiki/Data_Encryption_Standard - 83k -
Cached - Similar pages

DES - Wikipedia, the free encyclopedia
Data Encryption Standard, a method of **encryption;**
Diethylstilbestrol, a synthetic estrogen developed to supplement
a woman's natural estrogen production ...
en.wikipedia.org/wiki/DES - 14k - Cached - Similar pages

[PDF] FIPS 46-3, Data Encryption Standard (DES)
File Format: PDF/Adobe Acrobat - View as HTML
Key words: computer security, **data encryption standard,** triple **data
encryption** ... The X9.52 **standard,** "Triple **Data Encryption** Algorithm
Modes of Operation" ...
csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf - Similar pages

Triple DES, DES, and Skipjack - FIPS 46-3, 81, and 185
FIPS 46-3, **Data Encryption Standard** (DES), specifies the DES and Triple-DES
algorithms. For the complete specification of Triple-DES, the **standard** ANSI ...
csrc.nist.gov/cryptval/des.htm - 7k - Cached - Similar pages

What is Data Encryption Standard? - a definition from Whatis.com ...
Data Encryption Standard (DES) is a widely-used method of **data encryption** using a
private (secret) key that was judged so difficult to break by the US ...
searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213893,00.html - 83k -
Cached - Similar pages

What is DES? - A Word Definition From the Webopedia Computer ...
Short for **Data Encryption Standard**, a popular symmetric-key **encryption** method
developed in 1975 and standardized by ANSI in 1981 as ANSI X.3.92. ...
www.webopedia.com/TERM/D/DES.html - 48k - Cached - Similar pages

Data Encryption Standard (DES) - Free Computer Science Tutorials ...

Sponsored Links

Document Security w/Adobe
Protect & Secure Your Documents w/
LiveCycle Policy Server- Try Free.
www.Adobe.com

Data Encryption Standard
Strong Encryption. Any PC Worldwide.
Easy to Use. Guaranteed Protection.
secure.cypherix.co.uk

Data Encryption Standard
Searching for **data** encryptions?
Visit our **data** encryptions guide.
DataEncryptions.info

All the Data Encryption
All the **Data Encryption** Savings
Find Local **Data Encryption** Here!
Encryption.AlltheIndustrials.com

Data Encryption Standard
Up-to-the-Minute News, Reports &
Whitepapers in Protocols. Try it!
www.Computerworld.com

Information about the **Data Encryption Standard** (DES) and its JavaScript implementation.
www.laynetworks.com/des.htm - 83k - Cached - Similar pages

Data Encryption Standard: Definition and Much More from Answers.com
DES (communications) **data encryption standard** (biochemistry) diethylstilbesterol.
www.answers.com/topic/**data-encryption-standard** - 114k - Cached - Similar pages

[PDF] Standing the Test of Time: The **Data Encryption Standard**, Volume 47 ...
File Format: PDF/Adobe Acrobat - View as HTML
The workhorse private-key algorithm is the **Data. Encryption Standard** (DES), which relies
on cryp- ... reau of **Standards, Data Encryption Standard**, Fed- ...
www.ams.org/notices/200003/fea-landau.pdf - Similar pages

Result Page: 1 2 3 4 5 6 7 8 9 10   **Next**

Try Google Desktop: search your computer as easily as you search the web.

| data encryption standard | | Search |

Search within results | Language Tools | Search Tips | Dissatisfied? Help us improve

---

Google Home - Advertising Programs - Business Solutions - About Google

©2006 Google

P⬗RTAL

USPTO

Search: ⦿ The ACM Digital Library ○ The Guide

((cryptography engine) and (data block) and portion and (key|

SEARCH

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction survey

Terms used
cryptography engine and **data block** and **portion** and **key scheduler** and **sequence** and **inverse**

Found **58,104** of **192,876**

Sort results by: [relevance ▼]

Display results: [expanded form ▼]

🔖 Save results to a Binder

? Search Tips

☐ Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 200
Best 200 shown

Result page: **1** 2 3 4 5 6 7 8 9 10 next

Relevance scale ☐ ▭ ▣ ◼ ◼

1 Computing curricula 2001

September 2001 **Journal on Educational Resources in Computing (JERIC)**
Publisher: ACM Press
Full text available: 📄 pdf(613.63 KB) 💲 Additional Information: full citation, references, citings, index terms
html(2.78 KB)

2 Link and channel measurement: A simple mechanism for capturing and replaying wireless channels
Glenn Judd, Peter Steenkiste
August 2005 **Proceeding of the 2005 ACM SIGCOMM workshop on Experimental approaches to wireless network design and analysis E-WIND '05**
Publisher: ACM Press
Full text available: 📄 pdf(6.06 MB) Additional Information: full citation, abstract, references, index terms

Physical layer wireless network emulation has the potential to be a powerful experimental tool. An important challenge in physical emulation, and traditional simulation, is to accurately model the wireless channel. In this paper we examine the possibility of using on-card signal strength measurements to capture wireless channel traces. A key advantage of this approach is the simplicity and ubiquity with which these measurements can be obtained since virtually all wireless devices provide the req ...

Keywords: channel capture, emulation, wireless

3 Cryptography as an operating system service: A case study
Angelos D. Keromytis, Jason L. Wright, Theo De Raadt, Matthew Burnside
February 2006 **ACM Transactions on Computer Systems (TOCS)**, Volume 24 Issue 1
Publisher: ACM Press
Full text available: 📄 pdf(669.12 KB) Additional Information: full citation, abstract, references, index terms

Cryptographic transformations are a fundamental building block in many security applications and protocols. To improve performance, several vendors market hardware accelerator cards. However, until now no operating system provided a mechanism that allowed both uniform and efficient use of this new type of resource.We present the OpenBSD Cryptographic Framework (OCF), a service virtualization layer implemented inside the operating system kernel, that provides uniform access to accelerator functio ...

Keywords: Encryption, authentication, cryptographic protocols, digital signatures, hash functions

4 Enabling trusted software integrity
Darko Kirovski, Milenko Drinić, Miodrag Potkonjak
October 2002 **ACM SIGPLAN Notices , ACM SIGARCH Computer Architecture News , ACM**

SIGOPS Operating Systems Review , Proceedings of the 10th international conference on Architectural support for programming languages and operating systems ASPLOS-X, Volume 37 , 30 , 36 Issue 10 , 5 , 5

Publisher: ACM Press

Full text available: pdf(1.39 MB)   Additional Information: full citation, abstract, references, citings

Preventing execution of unauthorized software on a given computer plays a pivotal role in system security. The key problem is that although a program at the beginning of its execution can be verified as authentic, while running, its execution flow can be redirected to externally injected malicious code using, for example, a buffer overflow exploit. Existing techniques address this problem by trying to detect the intrusion at run-time or by formally verifying that the software is not prone to a p ...

5   Real-time shading

Marc Olano, Kurt Akeley, John C. Hart, Wolfgang Heidrich, Michael McCool, Jason L. Mitchell, Randi Rost

August 2004 **ACM SIGGRAPH 2004 Course Notes SIGGRAPH '04**

Publisher: ACM Press

Full text available: pdf(7.39 MB)   Additional Information: full citation, abstract

Real-time procedural shading was once seen as a distant dream. When the first version of this course was offered four years ago, real-time shading was possible, but only with one-of-a-kind hardware or by combining the effects of tens to hundreds of rendering passes. Today, almost every new computer comes with graphics hardware capable of interactively executing shaders of thousands to tens of thousands of instructions. This course has been redesigned to address today's real-time shading capabili ...

6   Architectural support for fast symmetric-key cryptography

Jerome Burke, John McDonald, Todd Austin

November 2000 **ACM SIGOPS Operating Systems Review , ACM SIGARCH Computer Architecture News , Proceedings of the ninth international conference on Architectural support for programming languages and operating systems ASPLOS-IX**, Volume 34 , 28 Issue 5 , 5

Publisher: ACM Press

Full text available: pdf(160.25 KB)   Additional Information: full citation, abstract, references, citings, index terms

The emergence of the Internet as a trusted medium for commerce and communication has made cryptography an essential component of modern information systems. Cryptography provides the mechanisms necessary to implement accountability, accuracy, and confidentiality in communication. As demands for secure communication bandwidth grow, efficient cryptographic processing will become increasingly vital to good system performance.In this paper, we explore techniques to improve the performance of symmetr ...

7   Special issue: AI in engineering

D. Sriram, R. Joobbani

April 1985   **ACM SIGART Bulletin**, Issue 92

Publisher: ACM Press

Full text available: pdf(8.79 MB)   Additional Information: full citation, abstract

The papers in this special issue were compiled from responses to the announcement in the July 1984 issue of the SIGART newsletter and notices posted over the ARPAnet. The interest being shown in this area is reflected in the sixty papers received from over six countries. About half the papers were received over the computer network.

8   System-level power optimization: techniques and tools

Luca Benini, Giovanni de Micheli

April 2000   **ACM Transactions on Design Automation of Electronic Systems (TODAES)**, Volume 5 Issue 2

Publisher: ACM Press

Full text available: pdf(385.22 KB)   Additional Information: full citation, abstract, references, citings, index terms

This tutorial surveys design methods for energy-efficient system-level design. We consider electronic sytems consisting of a hardware platform and software layers. We consider the three major constituents of hardware that consume energy, namely computation, communication, and storage units, and we review methods of reducing their energy consumption. We also study models for analyzing the energy cost of software, and methods for energy-efficient software design and compilation. This survery ...

9 Security on FPGAs: State-of-the-art implementations and attacks

Thomas Wollinger, Jorge Guajardo, Christof Paar

August 2004 **ACM Transactions on Embedded Computing Systems (TECS)**, Volume 3 Issue 3

Publisher: ACM Press

Full text available: pdf(296.79 KB)   Additional Information: full citation, abstract, references, index terms

In the last decade, it has become apparent that embedded systems are integral parts of our every day lives. The wireless nature of many embedded applications as well as their omnipresence has made the need for security and privacy preserving mechanisms particularly important. Thus, as field programmable gate arrays (FPGAs) become integral parts of embedded systems, it is imperative to consider their security as a whole. This contribution provides a state-of-the-art description of security issues ...

Keywords: Cryptography, FPGA, attacks, cryptographic applications, reconfigurable hardware, reverse engineering, security

10 Parallel execution of prolog programs: a survey

Gopal Gupta, Enrico Pontelli, Khayri A.M. Ali, Mats Carlsson, Manuel V. Hermenegildo

July 2001 **ACM Transactions on Programming Languages and Systems (TOPLAS)**, Volume 23 Issue 4

Publisher: ACM Press

Full text available: pdf(1.95 MB)   Additional Information: full citation, abstract, references, citings, index terms

Since the early days of logic programming, researchers in the field realized the potential for exploitation of parallelism present in the execution of logic programs. Their high-level nature, the presence of nondeterminism, and their referential transparency, among other characteristics, make logic programs interesting candidates for obtaining speedups through parallel execution. At the same time, the fact that the typical applications of logic programming frequently involve irregular computatio ...

Keywords: Automatic parallelization, constraint programming, logic programming, parallelism, prolog

11 PODS invited talk: Models and issues in data stream systems

Brian Babcock, Shivnath Babu, Mayur Datar, Rajeev Motwani, Jennifer Widom

June 2002 **Proceedings of the twenty-first ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems**

Publisher: ACM Press

Full text available: pdf(257.79 KB)   Additional Information: full citation, abstract, references, citings, index terms

In this overview paper we motivate the need for and research issues arising from a new model of data processing. In this model, data does not take the form of persistent relations, but rather arrives in multiple, continuous, rapid, time-varying *data streams*. In addition to reviewing past work relevant to data stream systems and current projects in the area, the paper explores topics in stream query languages, new requirements and challenges in query processing, and algorithmic issues.

12 Data and memory optimization techniques for embedded systems

P. R. Panda, F. Catthoor, N. D. Dutt, K. Danckaert, E. Brockmeyer, C. Kulkarni, A. Vandercappelle, P. G. Kjeldsberg

April 2001 **ACM Transactions on Design Automation of Electronic Systems (TODAES)**, Volume 6 Issue 2

Publisher: ACM Press

Full text available: pdf(339.91 KB)   Additional Information: full citation, abstract, references, citings, index terms

We present a survey of the state-of-the-art techniques used in performing data and memory-related optimizations in embedded systems. The optimizations are targeted directly or indirectly at the memory subsystem, and impact one or more out of three important cost metrics: area, performance, and power dissipation of the resulting implementation. We first examine architecture-independent optimizations in the form of code transoformations. We next cover a broad spectrum of optimizati ...

Keywords: DRAM, SRAM, address generation, allocation, architecture exploration, code transformation, data cache, data optimization, high-level synthesis, memory architecture customization, memory power dissipation, register file, size estimation, survey

13 Building a robust software-based router using network processors

Tammo Spalink, Scott Karlin, Larry Peterson, Yitzchak Gottlieb

October 2001 **ACM SIGOPS Operating Systems Review , Proceedings of the eighteenth ACM symposium on Operating systems principles SOSP '01**, Volume 35 Issue 5

Publisher: ACM Press

Full text available: pdf(1.49 MB)   Additional Information: full citation, abstract, references, citings, index terms

Recent efforts to add new services to the Internet have increased interest in software-based routers that are easy to extend and evolve. This paper describes our experiences using emerging network processors---in particular, the Intel IXP1200---to implement a router. We show it is possible to combine an IXP1200 development board and a PC to build an inexpensive router that forwards minimum-sized packets at a rate of 3.47Mpps. This is nearly an order of magnitude faster than existing pure PC-base ...

14 Automatic temporal layout mechanisms revisited

M. Cecelia Buchanan, Polle T. Zellweger

February 2005 **ACM Transactions on Multimedia Computing, Communications, and Applications (TOMCCAP)**, Volume 1 Issue 1

Publisher: ACM Press

Full text available: pdf(1.09 MB)   Additional Information: full citation, abstract, references, citings, index terms

A traditional static document has a spatial layout that specifies where objects in the document appear. Because multimedia documents incorporate time, they also require a temporal layout, or schedule, that specifies when events in the document occur. This article argues that multimedia document systems should provide mechanisms for automatically producing temporal layouts for documents. The major advantage of this approach is that it makes it easier for authors to create and modify multimedia do ...

Keywords: Multimedia documents, multimedia authoring, temporal formatting, temporal specification

15 The KaffeOS Java runtime system

Godmar Back, Wilson C. Hsieh

July 2005   **ACM Transactions on Programming Languages and Systems (TOPLAS)**, Volume 27 Issue 4

Publisher: ACM Press

Full text available: pdf(704.30 KB)   Additional Information: full citation, abstract, references, index terms

Single-language runtime systems, in the form of Java virtual machines, are widely deployed platforms for executing untrusted mobile code. These runtimes provide some of the features that operating systems provide: interapplication memory protection and basic system services. They do not, however, provide the ability to isolate applications from each other. Neither do they provide the ability to limit the resource consumption of applications. Consequently, the performance of current systems degra ...

Keywords: Robustness, garbage collection, isolation, language runtimes, resource management, termination, virtual machines

16 Anatomy of a native XML base management system

T. Fiebig, S. Helmer, C.-C. Kanne, G. Moerkotte, J. Neumann, R. Schiele, T. Westmann

December 2002 **The VLDB Journal — The International Journal on Very Large Data Bases**, Volume 11 Issue 4

Publisher: Springer-Verlag New York, Inc.

Full text available: pdf(300.97 KB)   Additional Information: full citation, abstract, citings, index terms

Several alternatives to manage large XML document collections exist, ranging from file systems over relational or other database systems to specifically tailored XML base management systems. In this paper we give a tour of Natix, a database management system designed from scratch for storing and processing XML data. Contrary to the common belief that management of XML data is just another application for traditional databases like relational systems, we illustrate how almost every component in a ...

Keywords: Database, XML

17 A high-speed network interface for distributed-memory systems: architecture and applications
Peter Steenkiste
February 1997 **ACM Transactions on Computer Systems (TOCS)**, Volume 15 Issue 1
Publisher: ACM Press
Full text available: pdf(993.12 KB)   Additional Information: full citation, abstract, references, index terms, review

> Distributed-memory systems have traditionally had great difficulty performing network I/O at rates proportional to their computational power. The problem is that the network interface has to support network I/O for a supercomputer, using computational and memory bandwidth resources similar to those of a workstation. As a result, the network interface becomes a bottleneck. In this article we present an I/O architecture that addresses these problems and supports high-speed network I/O on dist ...

> **Keywords**: I/O architecture, application-managed I/O, data reshuffling, distributed memory systems, network interface, outboard buffering, protocol processing, resource management

18 Courses: State of the art in interactive ray tracing
Peter Shirley
July 2006   **Material presented at the ACM SIGGRAPH 2006 conference SIGGRAPH '06**
Publisher: ACM Press
Full text available: pdf(14.08 MB)   Additional Information: full citation, abstract

> Recent improvements in computer hardware have allowed ray tracing to be used in some interactive applications. The trends in architecture and expansions of geometric model should increase the use of interactive ray tracing. This course presents recent and often not-yet published work on interactive ray tracing.

19 Retrospective on Aurora
Hari Balakrishnan, Magdalena Balazinska, Don Carney, Uğur Çetintemel, Mitch Cherniack, Christian Convey, Eddie Galvez, Jon Salz, Michael Stonebraker, Nesime Tatbul, Richard Tibbetts, Stan Zdonik
December 2004 **The VLDB Journal — The International Journal on Very Large Data Bases**, Volume 13 Issue 4
Publisher: Springer-Verlag New York, Inc.
Full text available: pdf(349.43 KB)   Additional Information: full citation, abstract, index terms

> This experience paper summarizes the key lessons we learned throughout the design and implementation of the Aurora stream-processing engine. For the past 2 years, we have built five stream-based applications using Aurora. We first describe in detail these applications and their implementation in Aurora. We then reflect on the design of Aurora based on this experience. Finally, we discuss our initial ideas on a follow-on project, called Borealis, whose goal is to eliminate the limitations of A ...

> **Keywords**: Data stream management, Distributed stream processing, Monitoring applications, Quality-of-service, Stream-processing engines

20 Embedded applications: AES and the cryptonite crypto processor
Dino Oliva, Rainer Buchty, Nevin Heintze
October 2003 **Proceedings of the 2003 international conference on Compilers, architecture and synthesis for embedded systems**
Publisher: ACM Press
Full text available: pdf(346.09 KB)   Additional Information: full citation, abstract, references, index terms

> CRYPTONITE is a programmable processor tailored to the needs of crypto algorithms. The design of CRYPTONITE was based on an in-depth application analysis in which standard crypto algorithms (AES, DES, MD5, SHA-1, etc) were distilled down to their core functionality. We describe this methodology and use AES as a central example. Starting with a functional description of AES, we give a high level account of how to implement AES efficiently in hardware, and present several novel optimizations (whic ...

> **Keywords**: AES, architecture, cryptography, high-bandwidth, high-speed, processor,

round key generation, software implementation

Results 1 - 20 of 200   Result page: **1**   2   3   4   5   6   7   8   9   10   next